UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/760,956	01/15/2001	Christopher L. Knauft	MEDIDNA.043A	4816

7590	08/25/2005

MacPherson Kwok Chen & Heid LLP
1762 Technology Dr.
Suite 226
San Jose, CA 95110

EXAMINER
TRAN, TONGOC

ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 08/25/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

	Application No.	Applicant(s)
Office Action Summary	09/760,956	KNAUFT, CHRISTOPHER L.
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 June 2005*.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-7,9-17,19-29,31-32,35-38,40-44-* is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-7,9-17,19-29,31,32,35-38 and 40-44* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some * c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *6/10/05*.

4)☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

1.   This office action is in response to Applicant's Request for Continued

Examination (RCE) filed on June 7, 2005. Claims 1-7, 9-17, 19-29, 31-32, 35-38 and

40-44 are pending.

Response to Arguments

2.   Applicant's arguments with respect to claims 1, 25, 32, 38 and 44 have been

considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-7, 9-17, 19-29, 31, 32, 35-38 and 40-44 are rejected under 35 U.S.C.

103(a) as being unpatentable over Sims, III (U.S. Patent No. 6,550,011) in view of

Abbott et al. (U.S. Patent No. 6,671,808, hereinafter Abbott).

In respect to claim 1, Sims discloses a user data processor for providing access

to a rights controlled data object, the user data processor comprising:

a processing device (col. 11, lines 5-15);

a communication; device connected to the processing device and configured to receive an encrypted secure package containing a portion of the rights controlled data object (see col. 1, lines 13-29);

a user program running on the processing device, the user program configured to control access to the rights controlled data object; a user program security module configured to at least partially decrypt the secure package using a user program key (see col. 9, lines 60-67); and

a machine key device connected to and associated with the processing device and accessible by the user program, the machine key device configured to restrict the use of the data object to the user data processor using a machine key (see col, 15, lines 18-34).

Sims discloses it is additionally possible to uniquely encrypt the content per user so that if unauthorized copies are made available or a secret key is published the source might be identified (Sims, col. 9, lines 60-67). However, Sims does not explicitly disclose but Abbott discloses a user device associated with a user, the user key device detachably connected to the processing device, accessible by the user program and configured to restrict the use of the data object to the user data processor using a machine key (see Abbott, col. 3, lines 25-63). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate the teaching of a user device associated with a user detachably connected to the processing device taught by Abbott with the teaching of additioanly encrypting the content per user taught

by Sims for the benefit of ensuring the identity of the user of the content (Abbott, col. 3,

lines 45-49).

In respect to claim 2, Sims and Abbott disclose the user data processor of Claim

1, wherein the user program is configured to communicate with the machine key device

to authenticate the identity of the processing device using the machine key (see Sims,

col. 15, lines 18-34).

In respect to claim 3, Sims and Abbott disclose the user data processor of Claim

2, wherein the processing device is configured to provide rights controlled access to

digital video (see Sims, col. 2, lines 1-3).

In respect to claim 4, Sims and Abbott disclose the user data processor of Claim

1, wherein the encrypted secure package is encrypted with at least the user program

key and the machine key, and wherein the machine key device is configured to at least

partially decrypt the secure package using the machine key (see Sims, Col. 12, lines

13-21).

In respect to claim 5, Sims and Abbott disclose the user data processor of Claim

4, wherein the user program is configured to communicate with the machine key device

to authenticate the identity of the processing device using the machine key (see Sims,

Col. 5, lines 18-38).

In respect to claim 6, Sims and Abbott disclose the user data processor of Claim

5, wherein the machine key is an asymmetric machine key pair comprising a public

machine key and a private machine key (see Sims, Col. 12, lines 13-21).

In respect to claim 7, Sims and disclose the user data processor of Claim 6, wherein the machine key device is configured to generate the asymmetric machine key pair (see Sims, Col. 14, line 58-col. 15, line 3).

In respect to claim 9, Sims and Abbott disclose the user data processor of Claim 8, wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key, and wherein the user program is configured to communicate with the user key device to authenticate the identity of the user using the user key (see Sims, Col. 12, lines 13-21).

In respect to claim 10, Sims and Abbott disclose the user data processor of Claim 8, wherein the encrypted secure package is encrypted with at least the user program key, the machine key, and the user key, wherein the machine key device is configured to at least partially decrypt the secure package using the machine key, and wherein the user key device is configured to at least partially decrypt the secure package using the user key (see Sims, col. 12, lines 13-21).

In respect to claim 11, Sims and disclose the user data processor of Claim 10, wherein the user program is configured to communicate with the machine key device to authenticate the identity of the processing device using the machine key, and wherein the user program is configured to communicate with the user key device to authenticate the identity of the user using the user key (see Sims, Col. 12, lines 13-21).

In respect to claim 12, Sims and Abbott disclose the user data processor of Claim 8, further comprising:

a second security module configured to at least partially decrypt the secure

package using a second key; and a third security module configured to at least partially

decrypt the secure package using a third key (see Sims, Col. 12, lines 13-21 and Col.

20, lines 31-43).

In respect to claim 13, Sims and Abbott disclose the user data processor of

Claim 12, wherein the second security module is configured to communicate with the

user key device to authenticate the identity of the processing device using the user key,

and wherein the third security module is configured to communicate with the machine

key device to authenticate the identity of the processing device using the machine key

(see Abbott, Col. 12, lines 13-21 and col. 20, lines 31-43).

In respect to claim 14, Sims and Abbott disclose the user data processor of

Claim 12, wherein the second key is a portion of the user key, wherein the second

security module is configured to obtain the second key from the user key device,

wherein the third key is a portion of the machine key, and wherein the third security

module is configured to obtain the third key from the machine key device (see Sims, col.

20,lines 31-43).

In respect to claim 15, Sims and Abbott disclose the user data processor of

Claim 14, wherein the second security module and the third security module are parts of

the user program (see Sims, col. 20, lines 31-43).

In respect to claim 16, Sims and Abbott disclose the user data processor of

Claim 1, further comprising a third security module configured to at least partially

decrypt the secure package using a third key (see Sims, col. 12, lines 13-21).

In respect to claim 17, Sims and Abbott disclose the user data processor of

Claim 16, wherein the third security module is configured to communicate with the

machine key device to authenticate the identity of the processing device using the

machine key (see Sims, 12, lines 13-21).

In respect to claim 19, Sims and Abbott disclose the user data processor of

Claim 16, wherein the third key is a portion of the machine key, and wherein the third

security module is configured to obtain the third key from the machine key device (see

Sims, col. 12, lines 13-21 and col. 20, lines 31-43).

In respect to claim 20, Sims and Abbott disclose the user data processor of

Claim 1, wherein the third security module is a part of the user program (see Sims, col.

20, lines 31-43).

In respect to claim 21, Sims and Abbott disclose the user data processor of

Claim 1, wherein the user program is implemented in hardware (see Sims, col. 4, line

63-col. 5, line 10).

In respect to claim 22, Sims and Abbott disclose the user data processor of

Claim 1, wherein the user program security module is part of the user program (see

Sims, col. 4, line 63-col. 5, line 10).

In respect to claim 23, Sims and Abbott disclose the user data processor of

Claim 1, wherein the processing device is a general purpose computer (see Sims, col.

3, lines 30-46).

In respect to claim 24, Sims and Abbott disclose the user data processor of

Claim 1, wherein the processing device and the machine key device are contained in a

single integrated circuit (see Sims, col. 12, lines 42-57).

In respect to claim 27, Sims and Abbott disclose the method of claim 26, further

comprising:

(H) digitally signing the control elements such that the control elements can be

authenticated; and (I) transmitting the digital signature of the controlled elements to the

user data processor (see Sims, col. 5, lines 39-59).

In respect to claims 25-26 and 28-29, 31, 32, 35-38 and 40-44, the claim

limitations are similar to claims 1-24 and 27. Therefore, claims 25-26 and 28-29, 31, 32,

35-38 and 40-44 are rejected based on the similar rationale.

4.   Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sims

(U.S. Patent No. 6,550,011) Abbott (U.S. Patent No. 6,671,808) and further in view of

Keeler, Jr. et al. (U.S. Patent No. 6,502,130, hereinafter Keeler).

In respect to claim 18, Sims and Abbott disclose the user data processor of

Claim 17. Sims and Abbott do not disclose the MAC address of the user data processor

is a key (see Keeler, cot. 4, lines 30-48). Therefore, it would have been obvious to one

of ordinary skill in the art at the time the invention was made to implement Sims and

Abbott's teaching of encrypting content with machine key and user key with Keeler's

teaching of using MAC address of the network system as a key so that it can

conveniently identify the source if unauthorized content is identified.

Conclusion

5.   Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Tongoc Tran whose telephone number is (571) 272-

3843. The examiner can normally be reached on 8:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number

for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the

Patent Application Information Retrieval (PAIR) system. Status information for

published applications may be obtained from either Private PAIR or Public PAIR.

Status information for unpublished applications is available through Private PAIR only.

For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic

Business Center (EBC) at 866-217-9197 (toll-free).

Examiner: Tongoc Tran
Art Unit: 2134

August 19, 2005

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100